March 2004 Federal Identity Credentialing Committee

Policy Issuance Regarding Smart Cards Systems For Identification and Credentialing of Employees

Background

E-Government, an integral part of the President's Management Agenda (PMA), is defined as the use of digital technologies to transform government operations in order to improve effectiveness, efficiency, and service delivery. As the Federal government modernizes internal processes and adopts cross-agency applications available to all Federal employees, a common, trusted basis for authenticating the identity of individuals within the Federal sector is required. The events of 11 September 2001 underlined the importance of this requirement. GAO has repeatedly found in tests since 9-11 that "government officials did not recognize that the documents [credentials] we presented were counterfeit." Additionally, in accordance with the President's vision of creating a more responsive and cost-effective government, the Office of Management and Budget provided a memo to Federal Chief Information Officers outlining details of the E-Authentication E-Government initiative on authentication and identity management (memo dated 3 July 2003, Subject: Streamlining Authentication and Identity Management within the Federal Government), which stipulated additional policy would be forthcoming.

Purpose and Applicability

This policy provides guidance on the use of smart card based technology in badge, identification, and credentialing systems within the Federal sector, with the objective of helping agencies plan, budget, establish and implement credentialing and identification systems for Federal government employees and their agents. This document applies specifically to the use of smart card based platforms in the credentialing and identification activities of Federal government employees, contractors and affiliates supporting Federal agencies.

Following the guidance set forth in this policy will lead to a robust, interoperable identity and authentication platform both for physical and logical access conducted on sensitive but unclassified networks. Successful planning and implementation in this area requires the support of all the Federal communities involved in credentialing and identification, including those involved in physical and cyber security, human resources management, and e-authentication.

This policy sets the direction for all agencies to deploy enterprise-wide, standards-based, interoperable smart card – based systems. This guidance should be applied to all Federal badge systems involving credentialing and identification systems, except those that are national security systems as defined in U.S.C. 3542(b)(2). This policy does not apply directly to authorization but to using a smart card platform capable of interoperability with other smart card – based systems. Decisions concerning authorization and privileges remain the purview of agencies and responsible security and facility officials. This policy encourages the use of smart cards for both physical and logical access, and emphasizes them for badge systems, whose primary purpose is for identification of employees and entry to Federal facilities and networks.

The primary intent of this policy is to eliminate inconsistent approaches to both physical and computer security, which lead to increased risks and redundant costs to the Federal government and the people with whom it interacts. This requires a common framework to enable cross-agency and government physical access capabilities as well as a migration path to incorporating logical access capability. In accordance with this approach, each agency will issue smart card-based credentials to its employees that meet the requirements of this policy, and develop the required supporting infrastructure for both physical and logical networks as current systems come up for replacement**.**

Each agency will issue identity credentials (smart cards) within its own domain in a secure manner to assure that each credential issued is bound to a person whose identity has been carefully vetted. Although issued individually by each agency, the end result must be a “trusted token” that can be made interoperable across the entire Federal enterprise. Interoperability includes the ability to have an individual’s identity electronically verified within the agency domain and across the federal enterprise for both physical and logical networks. The smart card-based identity credential will be the token used to establish (electronically read) an individual’s identity and provide the functionality for authentication of that person when challenged or required.

Robust Interoperable Identification Platform

In accordance with the President’s Management Agenda for e-Government and the Federal Identity Credentialing Framework, Federal agencies should begin planning for migrating their current access control systems, both physical and logical, in order to conform to this policy. Agencies should:

- Establish the issuance and deployment of an electronically readable credentialing smart card as the platform of choice for identity and authentication. For the purpose of this policy, the platform of choice will be a smart card that contains a contact and contactless integrated circuit chip. At the direction of the agency and in the short term, the platform may also incorporate other technologies on the card platform, as required to support legacy systems (e.g., magnetic stripe, bar code)

- Adopt standards for smart card and credentialing implementation that will permit interoperability of the smart card across all agency components as well as the entire Federal enterprise. Agencies needing a very robust card are encouraged to use an active “virtual machine” platform supporting multiple applications in accordance with both ISO/IEC 7816 and Global Platform specifications.

- Target a higher functionality threshold for credentialing employees and agents. This threshold should exceed existing credentialing systems today, which are based on a flash pass or card with, at most, PIN-based verification. A more robust credentialing functionality allows agencies to meet the need for identity and authentication for various threat levels and in disparate building and network infrastructures. This implies authentication methods beyond passwords for log-on to logical networks/applications, and methods beyond non-electronically-readable photo verification for physical access. The methods should include an active means of authentication for verification before access permissions are granted.

- Provide direction to component bureaus and entities requiring them to plan and budget based on principles of enterprise-wide implementation, use of standards-based systems components and interoperability. Such direction will help to maximize competition, minimize infrastructure costs, enable enterprise-wide interoperability of credentials, and improve security.

- Adopt practices that will ensure privacy while improving credentialing systems to improve security and promote efficiency of government business operations using standards-based technology. In the interest of protecting privacy of individuals, practices will also bar efforts to develop, or expand, existing databases for the purpose of tracking employee activity.

The Intent of Interoperability and setting the "Trust Model"

The intent for an interoperable, smart card-based Federal Agency Smart Credential (FASC) is to grant the attributes of "identity and a basic level of authentication" to a commonly accepted card across the entire Federal enterprise of sensitive but unclassified networks. As always, privileges granted to the bearer of the FASC is a local agency matter. The FASC is a core component to setting the "trust model" for these stated networks across the entire federal enterprise. It is intended that back end databases be updated to accept the credentials contained in the FASC. Agencies may invoke additional degrees of authentication beyond the FASC, as they deem appropriate for access control and liability purposes.

The FASC is to be used as the identity and basic authentication credential before an individual may gain access privileges for all work related and agency approved responsibilities within the *Issuing Agency*. It will be the basis of identity and basic authentication when visiting other domains within the federal government enterprise. It is intended that outside the issuing agency domain the FASC be recognized as the basis for identity and basic authentication by the *Relying Agency* and be the basis for granting access privileges without issuance of another identity card. The relying agency has the responsibility to verify the identity and validity status of the bearer of the FASC with the issuing agency as appropriate. The relying agency may issue additional logical credentials to the FASC issued by another agency if deemed necessary, but is required to seek approval of the issuing agency.

Binding the Identity to the FASC at Issuance

Issuance of the Federal Agency Smart Credential requires verification of end user identity prior to issuance. Each agency will employ an identity verification program prior to issuance of the FASC. The FASC will be acquired and issued in a secure process by the issuing agency that will include "In Person Proofing" that binds the "verified identity" of the intended bearer of the FASC to the credentials issued by the agency. The agency process will require that the bearer present breeder documentation that will be electronically verified and validated by the issuing agency in an in-person process prior to issuance of the FASC. The quantity and detail of breeder documentation required before issuance is agency dependent. Background investigations of criminal history, education certifications, credit history, work history, and so forth is at the discretion of each agency but at a minimum must meet current Office of Personnel Management (for Government employees) and Federal Acquisition Regulation (for contract agents) regulations. Individually identifiable data contained in background searches, resumes, and breeder documentation authenticity and verification must be kept secure, if stored, and meet agency privacy regulations

Agency Planning

Agencies should establish a smart card based identity and credentialing framework that:

- Assures that Federal suitability investigations are undertaken for all employees and contractors in accordance with Federal law and policy

- Adopts a clear and concise definition of terms so that all agencies have a common understanding and criteria for the trust model implemented by the issuing agency

- Drives trust of multi-agency credential tokens and credential information across the defined enterprise infrastructure. The system design must include a federated environment in order to determine with a high degree of confidence the identity, affiliated organization and credential entitlement of the guest credential (a credential presented from outside the agency). A federated approach takes into account how to deal with credential and token bearers from other issuers outside the facility being accessed

- Is driven by both Federal enterprise requirements as well as individual agency needs and includes recognition of the total cost of an access infrastructure for both physical and logical access. To maintain a common understanding of the latest developments, agencies are encouraged to participate in the scheduled meetings of the Federal Identity and Credentialing Committee (see www.cio.gov/ficc), the Smart Card Project Managers meetings, and the Smart Card Interagency Advisory Board (IAB) (see www.smart.gov)

- Converges disparate identity and authentication identity media (e.g. badges) to a common credential smart card used and trusted across the defined enterprise

- Is flexible enough to meet additional agency needs using legacy tokens until such time legacy systems are replaced and upgraded

- Safeguards individual rights to privacy

Common Credential Requirements for Smart Cards

Minimum requirements follow:

- Identity data must be in a standard electronically readable format and use an active authentication process.

- Information contained both on the visible surface of the Federal Agency Smart Credential and within the chip or chips will be tamper resistant and counterfeit-resistant. A tamper-resistant card contains features both making it difficult for persons to alter the information, and making alterations readily apparent to a qualified person or validating system. A counterfeit-resistant smart card contains features making it difficult for persons to produce illegitimate tokens that could be incorrectly accepted by a qualified person or validating system.

- Cards should support multiple authentication methods to protect the credential token from unauthorized use or theft. Factors may include something you know (e.g., a password), something you have in your possession (e.g., a digital certificate), and something you are (e.g., a biometric such as a fingerprint or iris scan). Agencies are encouraged to provide support for all these technologies in their architecture and planning.

- Smart cards must be supported by an infrastructure providing automated administration and maintenance of audit trails of smart card usage and must be in accordance with Electronic Records Management systems requirements

- Every smart card should have the capability to carry digital certificates for identity, encryption and digital signature. Credential requirements should be standards based meeting the certification requirements of the Federal Bridge model including all NIST recommended and approved standards and specifications such as FIPS 140-2: Security Requirements for Cryptographic Modules.

- Cards should have the capability to carry certificates needed to sign and encrypt sensitive mail as defined by the agency and be supported by agency applications.

- The card should allow post-issuance updating of data in a secure fashion and using a multi-factor means of authentication.

- The card should comply with NISTIR 6887, 2003 Edition – *Government Smart Card Interoperability Specification v2.1* (and later versions as they are issued) – identification formal standards, and other standards as appropriate

- Applications carried on the Federal Agency Smart Credential will be subjected to a certification process to ensure they are downloaded to the card in a secure and trusted manner and may require FIPS 140-2 validation. All applications or data downloaded to the Federal Agency Smart Credential are the responsibility of the issuing agency both at initial issuance and post issuance. The card should allow post-issuance updating of data in a secure fashion and using a multi-factor means of authentication.

- For security purposes agencies need to establish and enforce work policies and business processes that report a stolen or lost Federal Agency Smart Credential and revocation of privileges based on the Federal Agency Smart Credential as soon as possible. Agencies will also need to enter into agreements with other cooperating entities on procedures and methods to be developed for cross-agency notification when a credential is revoked or suspended.

As systems are replaced, agency components should replace present forms of identity and authentication media (e.g. badges) with the issuance of an electronically readable common smart card meeting the requirements of this policy.

Life Cycle Requirements

Agencies should plan for the entire life cycle of smart card based platforms, including the following functional components:

- Identity vetting – Identity vetting involves in-person proofing, and verification of authenticity and validity of breeder documentation. Identity vetting includes a process used to verify the identity of an individual via direct face-to-face validation of claimed identities and/or linkage to an authentication method. To assure identity in a trusted environment, agencies must address the specific issues of identity proofing and identity validation based on valid supporting documentation and, where possible, via the electronic verification and validation of the bearer's breeder documents (e.g., birth certificates and other basic documents user to obtain commonly obtained identity documents).

- Enrollment and registration – Enrollment is the process used to publish that a vetted individual has been sponsored by an organization. Once the individual's identity has been verified to an agreed upon assurance level, the individual will report to an enrollment station where a trusted agent will review that the individual's request has been processed correctly and completely. Registration is the process used to enter a vetted and enrolled individual into a security system. Agencies must develop policies that control and define the enrollment and registration processes.

- Card issuance – Card issuance is the process of distributing personalized cards to cardholders. Personalization entails both the logical and physical personalization of the card. Logical personalization involves transmittal and injection of the appropriate card applications, credentials, data, PIN and biometrics into the card application. Physical personalization encompasses printing of the physical characteristics and security features on the surface of the card. The personalization process is protected by controlled and highly secure methods. Agencies must develop policy guidance for card-processing requirements of initialization, personalization and fulfillment steps of card issuance based on applicable ISO, INCITS, FIPS, Global Platform and NIST standards and interoperability specifications.

- Card usage – The smart card is one of the most efficient authentication devices that can be used for both physical and logical access control applications. The smart card supports federated identity concepts, has trust characteristics that enable verification and validation of the integrity of credentials, and supports the risk-based management scheme of e-authentication. Agencies must provide policy guidance of how the card itself and credentials it stores can be used to provide necessary authentication levels for the access control of government facilities and services.

- Card revocation – For both physical and logical access controls, agencies must provide policy guidance of managing revocation of the card itself and credentials it stores.

- Post issuance updates or additions – Multi-application smart cards need to provide capabilities to add, delete and update card applications or data elements during the post-issuance phase of card life cycle. Agencies must define card configuration management and delegation of authority policies governing the creation, deletion, transfer and instantiation of card applications.

- Card reissuance and termination – The card reissuance process is used to provide replacements to individuals reporting a lost, stolen, or malfunctioning card. Generally when the card is reported lost, stolen, or malfunctioning, customer service deactivates the card by placing it on a "hot list." When a replacement card is issued, it must carry all the privileges, data, or and system access keys that resided on the original card that is being replaced. The termination process is used to permanently destroy or invalidate the usage of the card. Agencies must provide policy guidance for these processes.

Agencies should plan for a functional card life of six years.

Card Data Models

For smart card systems to work interoperably, it is important that agencies use common data models in a specified value format so that all Federal Agency Smart Credentials issued have the ability to be used throughout the federal enterprise, not just the agency's issuing domain. Card data models and specified value formats are defined in the most recent issuance of the *NISTIR 6887 – 2003 Edition, Government Smart Card Interoperability Specification (GSC-IS) v2.1*. It is at the discretion of each agency to select a data model for implementation before issuance. In accordance with the GSC-IS, the card capability container and an access control file for physical access is mandatory regardless of the data model selected. At this writing, agencies are working with the Government Smart Card Interagency Advisory Board (IAB) to develop a common minimum data model for use throughout the Federal enterprise.

Risk and Security Considerations

NIST is developing recommended technology solutions for four assurance levels for electronic transactions. Smart card systems must be developed to meet the requirements of the NIST Security Guidance Policy (not yet released at the time of this writing.) Physical security managers also need to develop risk-based approaches for badging policies related to physical access. Federal buildings are currently classified in four different categories, based on level or risk associated with attacks on buildings. Smart card systems should be considered for earlier implementation for facilities in the highest risk categories.

Biometric Technology

Agencies should design smart card systems that can support biometrics. Federal policy guidance is under development at this time and will be forthcoming. Biometrics adopted for use on smart cards must adhere to standards set by the American National Standards Institute (ANSI), InterNational Committee for Information Technology Standards (INCITS), the International Organization for Standardization (ISO), and the National Institute of Standards and Technology (NIST).

Other Guidance and Resources

For further information, background, and assistance in planning and implementing secure smart card – based identification systems, see the following:

Department of Homeland Security

- Office of Homeland Security, The White House, **"National Strategy for Homeland Security"**, dated 16 July 2002.

Department of Defense Common Access Card (CAC)

- DoD, Memorandum from John. J. Hamre, Deputy Secretary of Defense, **"Smart Card Adoption and Implementation"**, dated 10 November 1999.
- DoD, **"Common Access Card Execution Plan"**, 14 July 2000
- DoD, **"Configuration Management Plan for the Common Access Card"**, VI.1, 23 October 2000.
- DoD, DMDC/ACO and DON CIO, **"Common Access Card Release 1.0 ICC Requirements"**, final version 1.1, dated 8 February 2001.
- DoD, A Study by the Security Equipment Integration Working Group (SEIWG), **"Development of a specification for SEIWG-compliant Access Control Components"**, final dated 30 September 2002.

General Accounting Office

- GAO Testimony Before the Senate Committee on Finance, **"Security: Counterfeit Identification and Identification Fraud Raise Security Concerns"**, September 9, 2003, GAO-03-1147T.
- GAO Report to the Honorable Kay Bailey Hutchison, U.S. Senate, **"Aviation Security – Registered Traveler Program Policy and Implementation Issues"**, GAO-03-253 dated November 2002.
- GAO Report to the Chairman, Subcommittee on Technology and Procurement Policy, U.S. House of Representatives, **"Electronic Government – Progress in Promoting Adoption of Smart Card Technology",** GAO-03-144 draft version dated November 2002.
- GAO Report to Chairman, Subcommittee on Legislative Branch (Committee on Appropriations U.S. Senate), **"Technology Assessment – Using Biometrics for Border Security"**, GAO-03-174 dated November 2002.

- GAO Report to Congressional Requesters, **"BUILDING SECURITY – Security Responsibilities for Federally Owned and Leased Facilities"**, GAO—3-8 dated October 2002.

- GAO Report to the Chairman, Subcommittee on Government Efficiency, Financial Management and Intergovernmental Relations, Committee on Government Reform, House of Representatives, **"INFORMATION SECURITY – Advances and Remaining Challenges to Adoption of Public Key Infrastructure Technology"**, GAO-01-277 dated February 2001.

- GAO Testimony before the Subcommittee on Government Efficiency, Financial Management, and Intergovernmental Relations, Committee on Government Reform, House of Representatives**, "HOMELAND SECURITY –Effective Intergovernmental Coordination Is Key to Success",** dated 22 August 2002.

- GAO Testimony before the Subcommittee on Technology and Procurement Policy, Committee on Government Reform, House of Representatives, **"NATIONAL PREPAREDNESS – Technologies to Secure Federal Buildings"**, GAO-02-687T dated 25 April 2002.

General Services Administration

- General Services Administration, **"GSA Smart Card Handbook",** dated March 2004.

- Physical Access Interoperability Working Group (PAIWG), **"Government Smart Card Interoperability User Requirements for Physical Access using Contactless Technology"**, Working Draft dated October 2002.

- Physical Access Interoperability Working Group (PAIWG), Security Model Sub-Group, **"Physical Access Control Security Model"**, version 1.0 Final Draft dated November 2002.

- General Services Administration, Interagency Identification and Credentialing Policy Work Group (IICPWG), **"Scope and Tasking"**, version 11.0 dated 31 October 2002.

Office of Management and Budget

- OMB Policy Memorandum of July 3, 2003

- OMB Circular A-130, **"Management of Federal Information Resources"**

- OMB Memorandum, M-00-07, **"Incorporating and Funding Security in Information systems Investments"**, 28 February 2000.

- OMB Circular A-130, Appendix I, **"Federal Agency Responsibilities for Maintaining Records About Individuals".**

- OMB Circular A-130, Appendix III, **"Security of Federal Automated Information Resources"**.

- OMB, Memorandum M-00-10, **"OMB Procedures and Guidance on Implementing the Government Paperwork Elimination Act"**, 25 April 2002.

- OMB**,** Memorandum M-04-04 **"E-Authentication Guidance for Federal Agencies"**, 16 December 2003.

Department of Homeland Security – Transportation Security Administration

- Transportation Security Administration, CIWG, "Claimed Identity Working Group – Final Report", dated November 2002.

- Federal Aviation Administration, "FAA Smart Card Technical Report", dated June 2002.

- Transportation Security Administration, Credential Program Office, business case for "Transportation Worker Identification Credential (TWIC) High Level Concept of Operations", dated 5 November 2002.

- Federal Aviation Administration, "X.509 Certificate Policy", version 0.001 dated 26 November 2002.

Department of Transportation

- Department of Transportation (DOT) Handbook, DOT H 1350.2, **"Departmental Information Resources Management Manual (DIRMM)"**.

- Transportation Security Administration, CIWG, "**Claimed Identity Working Group – Final Report"**.

- Federal Aviation Administration, **"FAA Smart Card Technical Report"**, dated June 2002.

- Transportation Security Administration, Credential Program Office, **“Transportation Worker Identification Credential (TWIC) High Level Concept of Operations”**, dated 5 November 2002.

- Federal Aviation Administration, **“X.509 Certificate Policy”**, version 0.001 dated 26 November 2002.

National Institute of Standards and Technology

- NIST Internal Report 6887, **“Government Smart Card Interoperability Specification”**, version 2.1 dated 16 July 2003.

- NIST Assurance Level Technical Guidance reference (not released at the time of this writing).

National Research Council

- Stephen T. Kent and Lynette I. Millett, Editors on behalf of the Committee on Authentication Technologies and Their Privacy Implications of the National Research Council, **“IDs – Not That Easy --- Questions About Nationwide Identity Systems”**, Copyright 2002 by the National Academy of Sciences.

Industry Publications

- Smart Card Alliance, White Paper titled “**Secure Personal Identification System Policy, Process and Technology Choices for a Privacy-Sensitive Solution”**, January 2002.

- Smart Card Alliance, White Paper, **“Contactless Technology for Secure Physical Access: Technology and Standards Choices”**, October 2002.

- Liberty Alliance Project, **“Liberty Architecture Overview”**, version 1.1 -04 dated 15 November 2002.

Legislation

- Maritime Transportation Security Act (MTSA) 2002
- Clinger-Cohen Act (P.L. 104-106) Section 5113
- Federal Information Security Management Act (P.L. 107-347) Section 3544(a)
- E-Government Act (P.L. 104-347) Section 203
- The Government Paperwork Elimination Act (P.L. 105-277)
- The Homeland Security Act. 2002
- National Strategy for Homeland Security, OHS 2002

- The Enhanced Border Security and Visa Entry Reform Act, 2002
- The Port and Maritime Security Act, 2001
- The Aviation and Transportation Security Act, 2001
- USA Patriot Act, 2001
- The Electronic Signatures Act, 2000
- The Government Information Security Reform Act (GISRA), 1999
- OMB A-130: Management of Federal Information Resources, 1996
- The Information Technology Management Reform Act, 1996
- The Government Paperwork Reduction Act (PRA), 1995 The Privacy Act, 1974
- Information Sharing and the Privacy Act

Other

- See www.smart.gov for other resources

- See Smart Card Alliance web site (www.smartcardalliance.org) papers on smart card practices including those on: secure physical access, Contactless payments, privacy and smart cards, smart cards and retail payments, smart card reader catalog, Contactless technology, smart cards and biometrics, secure personal ID resources, and digital security initiative.

- See policy statements on biometrics at the International Biometrics Industry Association web site at www.ibia.org

- See International Labour Conference Provisional Record 20 of the 91st Session in Geneva, which outlines a good base of identity requirements for seamen (www.ilo.org/public/english/standards/ relm/ilc/ilc91/pdf/pr-20p2.pdf).

Updated 18Mar04